REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY) 22-10-2012	2. REPORT TYPE Final Report	3. DATES COVERED (From - To) 29-Sep-2011 - 28-Sep-2013

4. TITLE AND SUBTITLE
Automatic Identification & Mitigation of Unauthorized
Information Leaking from Tactical Mobile Networks

5a. CONTRACT NUMBER

5b. GRANT NUMBER
W911NF-11-C-0275

5c. PROGRAM ELEMENT NUMBER
1520BO

6. AUTHORS
Chris Greamo

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES
Invincea Labs, LLC
Invincea Labs, LLC
3975 University Drive, Suite 460
Fairfax, VA 22030 -2533

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSOR/MONITOR'S ACRONYM(S)
ARO

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
60726-CS-ST3.1

12. DISTRIBUTION AVAILABILITY STATEMENT
Approved for Public Release; Distribution Unlimited

13. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT

Most hand-held mobile devices today are equipped with a phone, web browser, music player, camera, and a horde of other applications and services. Google Android, NeoFreeRunner, Nokia Maemo, iPhone OS and Windows Phone OS are noteworthy hand-held device platforms capable of performing most of the functions previously found only in full-fledged desktop operating systems. Usability of such devices is further increased by the availability of third-party applications that can be purchased or freely downloaded by users from online application stores or

15. SUBJECT TERMS
Android, Tactical Mobile Networks, Mobile Security

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON Anup Ghosh
a. REPORT UU	b. ABSTRACT UU	c. THIS PAGE UU	UU		19b. TELEPHONE NUMBER 703-993-4776

Report Title

Automatic Identification & Mitigation of Unauthorized Information Leaking from Tactical Mobile Networks

ABSTRACT

Most hand-held mobile devices today are equipped with a phone, web browser, music player, camera, and a horde of other applications and services. Google Android, NeoFreeRunner, Nokia Maemo, iPhone OS and Windows Phone OS are noteworthy hand-held device platforms capable of performing most of the functions previously found only in full-fledged desktop operating systems. Usability of such devices is further increased by the availability of third-party applications that can be purchased or freely downloaded by users from online application stores or developer websites. Unfortunately, few of these applications provide the required level of security to protect the sensitive, potentially mission critical data that they access and store. Furthermore, while the major mobile device manufactures have given much lip service to security for their respective platforms, all currently fall way short of providing the robust security controls required to securely operate these devices in a tactical or other mission critical environment. This issue is under scored by the fact that no DoD accreditation authority has yet to accredit and authorize the use of any commercial mobile devices in a tactical environment despite the need and demand for the capabilities that such devices provide for the warfighter.

Enter List of papers submitted or published that acknowledge ARO support from the start of the project to the date of this printing. List the papers, including journal references, in the following categories:

(a) Papers published in peer-reviewed journals (N/A for none)

Received	Paper

TOTAL:

Number of Papers published in peer-reviewed journals:

(b) Papers published in non-peer-reviewed journals (N/A for none)

Received	Paper

TOTAL:

Number of Papers published in non peer-reviewed journals:

(c) Presentations

Number of Presentations: 0.00

Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

Received	Paper

TOTAL:

Number of Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

Peer-Reviewed Conference Proceeding publications (other than abstracts):

Received	Paper

TOTAL:

Number of Peer-Reviewed Conference Proceeding publications (other than abstracts):

(d) Manuscripts

Received	Paper

TOTAL:

Number of Manuscripts:

Books

Received	Paper

TOTAL:

Patents Submitted

Patents Awarded

Awards

Graduate Students

NAME PERCENT_SUPPORTED

FTE Equivalent:

Total Number:

Names of Post Doctorates

NAME PERCENT_SUPPORTED

FTE Equivalent:

Total Number:

Names of Faculty Supported

NAME PERCENT_SUPPORTED

FTE Equivalent:

Total Number:

Names of Under Graduate students supported

NAME PERCENT_SUPPORTED

FTE Equivalent:

Total Number:

Student Metrics

This section only applies to graduating undergraduates supported by this agreement in this reporting period

The number of undergraduates funded by this agreement who graduated during this period: 0.00

The number of undergraduates funded by this agreement who graduated during this period with a degree in science, mathematics, engineering, or technology fields:...... 0.00

The number of undergraduates funded by your agreement who graduated during this period and will continue to pursue a graduate or Ph.D. degree in science, mathematics, engineering, or technology fields:...... 0.00

Number of graduating undergraduates who achieved a 3.5 GPA to 4.0 (4.0 max scale):...... 0.00

Number of graduating undergraduates funded by a DoD funded Center of Excellence grant for Education, Research and Engineering:...... 0.00

The number of undergraduates funded by your agreement who graduated during this period and intend to work for the Department of Defense 0.00

The number of undergraduates funded by your agreement who graduated during this period and will receive scholarships or fellowships for further studies in science, mathematics, engineering or technology fields: 0.00

Names of Personnel receiving masters degrees

NAME

Total Number:

Names of personnel receiving PHDs

NAME

Total Number:

Names of other research staff

NAME	PERCENT_SUPPORTED
Mike Lack	0.40
FTE Equivalent:	**0.40**
Total Number:	**1**

Sub Contractors (DD882)

Inventions (DD882)

Scientific Progress

Our research was integrated in the Secure Android platform developed for DARPA's Transformative Apps program, and had to be aligned with the program's research and experimentation schedule. Within those constraints, this section highlights the key research results we achieved against our proposed work plan.

Tasks 1 & 2: SBU Wireless Comms (R & D, Impl & Support)

Unfortunately, the SBU Wireless communication research on the Transformative Apps program was delayed. Once the initial framework was in-place, we had expended all of our initial funding on this effort researching other tasks. We did however, leverage our Phase II research to inform the design of the SBU wireless architecture, adding the requirement that the Android HH device only connect to wireless networks that it is able to interrogate and identify as a valid, approved network.

Task 3: Handheld Security Stack

We successfully transitioned our Phase II authentication research into multiple facets of the Android security stack on the Transformative Apps program. The data-at-rest and zeroization functionality is provided by a native service on the Android device that interfaces with both a logon program (large keyboard) and a zeroization program that can be launched by users in the event of a device compromise. To prevent against denial-of-service by potential rogue applications, we implemented a challenge/response protocol within this native service to ensure that only authorized apps can call those services. Additionally, to control which applications are allowed on the device, we extended the existing, non-secure Android signature verification with a more robust challenge mechanism in which the Android Package Manager queries an application's manifest for specific information that could only be supplied by a program authorized mobile app. This capability has facilitated experimentation in Afghanistan, where the potential utility of different apps is evaluated. Our challenge/response mechanism has allowed for temporary (i.e. one week) endorsement of apps for evaluation. Finally, as well be described below, we added active challenge mechanisms to the USB stack on the Android handheld device.

Task 4: Laptop Security Stack

The most fruitful transition of the Phase II research was in securing the USB connection between the tactical handheld device and a laptop computer. Figure 1 below illustrates stock, unmodified USB communications between and Android handheld device and Windows PC.As can be seen, there is no authentication built into the communications mechanisms, allowing for the free exchange of (potentially sensitive) data between any Windows PC and any Android device either through USB Mass Storage or over the Android Debug Bridge (ADB) protocol. The only safeguards are user supplied settings and interactions on the Android device to enable these protocols.

For this effort, we applied the active challenge approach developed in Phase II to the problem of USB mutual authentication, ensuring that data can only be exchanged between authorized Windows PC's and authorized Android handheld devices. Figure 2 below illustrates the modifications we made to the USB communications stack under this effort.

Technology Transfer

invincea™

Automatic Identification & Mitigation of Unauthorized Information Leaking from Tactical Mobile Networks

Final Progress Report

October 22, 2012

DETECTION | PREVENTION | INTELLIGENCE

3975 University Drive, Suite 460, Fairfax, Virginia 22030 | (703) 352-7680 | Invincea.com | @invincea

Problem Statement

With the pervasiveness of high-speed wireless Internet access, robust computing power, and an endless stream of new mobile apps in the Android Marketplace and Apple App Store, mobile wireless devices are now the go-to computing device for a myriad of users including the warfighter. Commercial enterprises and the military alike are now facing the reality that these devices are not only being brought into and connected to sensitive networks, but are also being used for legitimate commercial business, work flow, and military mission applications. These new hand-held devices are capable of carrying significant amount of sensitive data. Not surprisingly, these devices are starting to become a prime target for those wishing to gain unauthorized access to such information.

Most hand-held mobile devices today are equipped with a phone, web browser, music player, camera, and a horde of other applications and services. Google Android, NeoFreeRunner, Nokia Maemo, iPhone OS and Windows Phone OS are noteworthy hand-held device platforms capable of performing most of the functions previously found only in full-fledged desktop operating systems. Usability of such devices is further increased by the availability of third-party applications that can be purchased or freely downloaded by users from online application stores or developer websites. Unfortunately, few of these applications provide the required level of security to protect the sensitive, potentially mission critical data that they access and store. Furthermore, while the major mobile device manufactures have given much lip service to security for their respective platforms, all currently fall way short of providing the robust security controls required to securely operate these devices in a tactical or other mission critical environment. This issue is under scored by the fact that no DoD accreditation authority has yet to accredit and authorize the use of any commercial mobile devices in a tactical environment despite the need and demand for the capabilities that such devices provide for the warfighter.

Summary of Results

Our research was integrated in the Secure Android platform developed for DARPA's Transformative Apps program, and had to be aligned with the program's research and experimentation schedule. Within those constraints, this section highlights the key research results we achieved against our proposed work plan.

Tasks 1 & 2: SBU Wireless Comms (R & D, Impl & Support)

Unfortunately, the SBU Wireless communication research on the Transformative Apps program was delayed. Once the initial framework was in-place, we had expended all of our initial funding on this effort researching other tasks. We did however, leverage our Phase II research to inform the design of the SBU wireless architecture, adding the requirement that the Android HH device only connect to wireless networks that it is able to interrogate and identify as a valid, approved network.

Task 3: Handheld Security Stack

We successfully transitioned our Phase II authentication research into multiple facets of the Android security stack on the Transformative Apps program. The data-at-rest and zeroization functionality is provided by a native service on the Android device that interfaces with both a logon program (large keyboard) and a zeroization program that can be launched by users in the event of a device compromise. To prevent against denial-of-service by potential rogue applications, we implemented a challenge/response protocol within this native service to ensure that only authorized apps can call those services. Additionally, to control which applications are allowed on the device, we extended the existing, non-secure Android signature verification with a more robust challenge mechanism in which the Android Package Manager queries an application's manifest for specific information that could only be supplied by a program authorized mobile app. This capability has facilitated experimentation in Afghanistan, where the potential utility of different apps is evaluated. Our challenge/response mechanism has allowed for temporary (i.e. one week) endorsement of apps for evaluation. Finally, as well be described below, we added active challenge mechanisms to the USB stack on the Android handheld device.

Task 4: Laptop Security Stack

The most fruitful transition of the Phase II research was in securing the USB connection between the tactical handheld device and a laptop computer. Figure I below illustrates stock, unmodified USB communications between and Android handheld device and Windows PC.

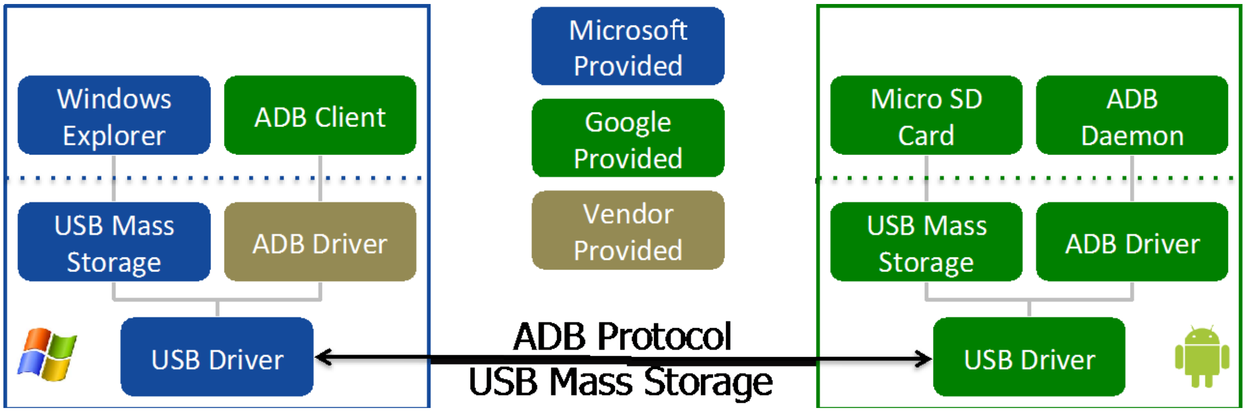

Figure 1 Standard Android USB Communication

As can be seen, there is no authentication built into the communications mechanisms, allowing for the free exchange of (potentially sensitive) data between any Windows PC and any Android device either through USB Mass Storage or over the Android Debug Bridge (ADB) protocol. The only safeguards are user supplied settings and interactions on the Android device to enable these protocols.

For this effort, we applied the active challenge approach developed in Phase II to the problem of USB mutual authentication, ensuring that data can only be exchanged between authorized Windows PC's and authorized Android handheld devices. Figure 2 below illustrates the modifications we made to the USB communications stack under this effort.

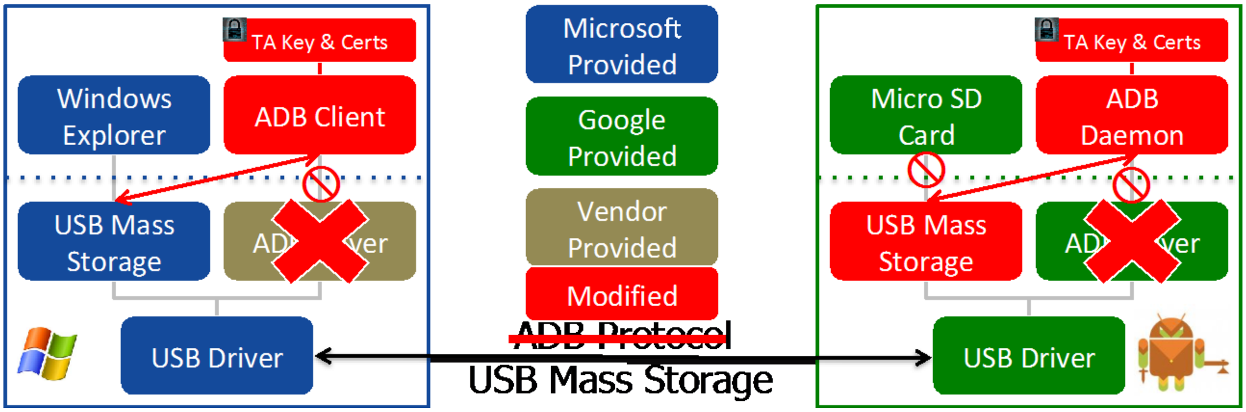

Figure 2 USB Mutual Authentication

As can be seen, we first focused on narrowing the communications protocols allowed over USB. Rather than leveraging the un-vetted, vendor supplied ADB USB transport, we instead focused on using USB Mass Storage as our transport mechanism. When a hardened Android device is connected to a Windows PC, it appears as an empty, read-only USB drive. At the transport layer, we built in an active challenge mechanism through the use of SCSI-generic vendor commands that are part of the USB Mass Storage specification. Through a series of specialized commands that only authorized devices know, an initial connection is made. Once the devices are connected, we then perform two additional authentication steps. The first is a cryptographic mutual authentication, using the FIPS 196 Public Key Entity Authentication protocol, where each device (PC and handheld) generate, encrypt and sign challenge problems and exchange them. The certificates and private keys are bound to each device through unique hardware identification mechanisms and validated to ensure that keys were not copied to an authorized device. Once the devices have authenticated cryptographically, the Android handheld then puts out a password challenge, requiring the user on the PC to enter the device's lockscreen password. If all authentications pass successfully, the devices can then begin exchanging data via the USB connection.

Task 5: Handheld Provisioning

To support the ongoing Transformative Apps experiments and pilots in Afghanistan, we transitioned the active challenge approach developed in Phase II to the secure, mass provisioning of Android handheld devices. The existing approach relied on techniques developed by the Android community to backup and restore Android devices through the recovery software mechanism. Basically, one Android device was built and configured, and then cloned onto additional devices to be fielded. As part of this effort, we enhanced that approach, building in cryptographic challenges into the back-up files themselves, along with modifying the recovery software on the Android device to trigger these responses. This approach ensures that only authorized Android back-ups produced by the Transformative Apps team can be restored onto a handheld device.